UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,192	10/21/2003	Brant L. Candelore	80398P558X	3671

8791 7590 03/04/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
03/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/690,192	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-32 are pending in this application.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/23/2008 has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. **Claims 1-14, 18, 10-13, 18-23, 27 and 28** are rejected under 35 U.S.C. 102(b) as being anticipated by **Kocher et al. (US 6,289,455)**, hereafter "Kocher".

Considering **Claim 1, 13, 22, and 28,** Kocher discloses a descrambler (Fig. 2) comprising: a memory to store a unique key (column 11- lines 27-30); a control word key ladder logic coupled to the memory (column 11- lines 6-65), the control word ladder logic comprising a first process block configured to generate a first derivative key of the unique key (column 11- lines 13-32, rights key), a second process block configured to generate a mating key from a mating key generator using the first derivative key (column 11- 35-45, KDM), and a third process block configured to recover a control word by decrypting an encrypted control word using the mating key (column 11- lines 51-56, CDK); a first cryptographic unit coupled to the control word key ladder logic (Fig. 2); the first cryptographic unit to descramble incoming content in a scrambled format using the control word (column 11- lines 60-65).

Considering **Claims 2, 3, 14, and 23,** Kocher discloses the descrambler of claim 1 being a single integrated circuit or a set-top-box (Fig. 2 – item 225 and item 210, column 22- lines 6-9).

Considering **Claim 4,** Kocher discloses the first value is a derivative key generated by performing a decryption operation on the CA random value using the unique key (column 11- lines 13-32).

Considering **Claim 5,** Kocher discloses the first value is a derivative key derived by performing a decryption operation on a combination of the CA random value and padding data (column 11- lines 13-32), the combination being at least 128-bits in length (column 14- lines 43-47, Fig. 8).

Considering **Claims 6 and 7,** Kocher discloses the second value is a mating key recovered by performing a decryption operation on a mating key generator using the

derivative key (column 11- lines 35-56) the mating key generator being a message comprising one or more of the following: a manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number (column 11- lines 35-45).

Considering **Claims 8 and 9,** Kocher discloses the third value is a control word recovered by performing a decryption operation on an encrypted control word using the mating key (column 11- lines 60-65, column 13- lines 54-58).

Considering **Claim 10,** Kocher discloses a third cryptographic unit to encrypt the descrambled incoming content prior to transmission to a digital device (Fig. 2- item 225 and item 215).

Considering **Claim 11,** Kocher discloses a copy protection ladder logic to produce a copy protection key used by the third cryptographic unit to encrypt the descrambled incoming content (column 12- lines 8-57, column 27- lines 40-47).

Considering **Claim 12,** Kocher discloses the copy protection ladder logic to produce a copy protection key by performing a decryption operation on a concatenation of a random value and a plurality of bits to produce a result being at least 128-bits in length, using a logical derivation being a result of an Exclusive OR (XOR) operation of the unique key and a predetermined value (column 12- lines 8-57, column 13- lines 33-41).

Considering **Claim 18,** Kocher discloses a copy protection ladder logic to produce a copy protection key based on a plurality of process blocks (column 12- lines 8-57), wherein a first process block configured to generate a derivative key based on a second random value and either the unique key or a logical derivation of the unique key

(column 12- lines 24-32), a second process block configured to recover a user key from an encrypted user key using the derivative key (column 12- lines 32-40), and a third process block configured to generate a copy protection key from a copy protection key generator using the user key (column 12- lines 50-57).

Considering **Claim 19 and 27,** Kocher discloses a third cryptographic unit to encrypt the descrambled incoming content using the copy protection key prior to transmission to a digital device (column 27- lines 40-47).

Considering **Claim 20 and 21,** Kocher discloses a one-time programmable, non-volatile memory coupled to the control word key ladder logic and the copy protection ladder logic, the non-volatile memory to store the unique key (Fig. 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claim 26 and 29** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kocher.**

Considering **Claim 26,** Kocher does not explicitly disclose a copy protection ladder logic coupled to the first cryptographic unit, the copy protection ladder logic comprising a fourth process block configured to generate a second derivative key based on a random value and the unique key; a fifth process block configured to decrypt an

encrypted user key using the second derivative key to recover a user key; and a sixth process block configured to generate a copy protection key from a copy protection key generator using the user key (column 13- Multiple Targeting, Batch Keys).
It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Kocher by adding a 4th-6th process block for the benefit of further encrypting the data and increasing the security of the unit and allowing for the reduction of REM messages, therefore, saving bandwidth.

Considering **Claim 29,** is rejected for the same reasons as claim 1 stated above. The ability to create a first key makes it obvious to create a second and third key using the same logic.

3. Claims 15-17, 24, 25, 30, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kocher in view of Wasilewski (US 2004/003008),** hereafter "Wasilewski".

Considering **Claims 15 and 24,** Kocher does not explicitly disclose a second cryptographic unit to decrypt incoming encrypted program data received out-of-band by a digital device implemented with the descrambler.
Wasilewski discloses a second cryptographic unit to decrypt incoming encrypted program data received out-of-band by a digital device implemented with the descrambler ([0013]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kocher by encrypting data received out-of-band as taught by Wasilewski in order to encrypt incoming authorization information ([0013]).

Considering **Claim 16, 17, and 25,** the combination of Kocher and Wasilewski discloses the encrypted program data comprises an encrypted entitlement management message that comprises at least two of (i) a smart card identifier, (ii) a length field, (iii) a mating key generator, (iv) at least one key identifier and (v) at least one key associated with the at least one key identifiers (Kocher- column 8- lines 45-51, column 11- lines 12-17).

Considering **Claim 30,** is rejected for the same reasons as claims 13-16 stated above. The ability to perform the same transformation multiple times would have been obvious to one of ordinary skill in the art.

Considering **Claim 31,** is rejected for the same reasons as claims 22-27 stated above. The ability to perform the same transformation multiple times would have been obvious to one of ordinary skill in the art.

Considering **Claim 32,** the combination of Kocher and Wasilewski discloses the bitwise logical operation is an Exclusive OR operation (Kocher- Fig. 8).

Response to Arguments

Applicant's arguments filed 12/23/2008 have been fully considered but they are not persuasive.

Regarding **Claims 1, 13, 22, and 28,** applicant's arguments have been fully considered but are not persuasive. With respect to applicants argument that Kocher fails to teach *a second process block configured to generate a mating key from a mating*

key generator using the first derivative key, the mating key generator being a message

that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number. Applicant is directed to Kocher- column 11, lines 35-65, Fig. 2. Kocher discloses:

> FIG. 5 shows an exemplary method of the present invention for deriving CDKs using rights keys stored in the CryptoFirewall's protected memory. At step 500, the interface control processor (ICP) receives a key derivation message (KDM) from the playback device. At step 510, the ICP uses the KDM to obtain a CDK generator value. (The CDK generator is typically an encrypted form of the CDK and is part of the KDM.)

The rights keys (i.e. first derivative keys) are used to derive the CDK's which are a part of the KDM (i.e. mating key). Therefore, Kocher discloses the first derivative key is used to generate a mating key. Kocher further discloses the rights key includes a content identifier.

With respect to applicant's argument that Kocher fails to teach *a third process block configured to recover a control word by decrypting an encrypted control word using the mating key*. Applicant is directed to Kocher- column 11, lines 48-65. Kocher discloses:

> The KDM also can identify which rights key is appropriate for processing each CDK generator.) At step 520, the CryptoFirewall verifies that the address is valid, then, at step 530, retrieves the corresponding value (the rights key) from the protected memory. At step 550, the CryptoFirewall uses pseudoasymmetric function F.sub.3, keyed with the rights key that was read from the protected memory at step 530, to transform the CDK generator. (In an alternate embodiment, F.sub.3 can be keyed with the CDK generator and used to transform the rights key itself. Also, F.sub.3 does not necessarily need to be a pseudoasymmetric or invertable function. For example, F3 can be a hash) At step 560, the CryptoFirewall returns the transformation result to the ICP. At step 570, the ICP optionally performs any final processing required to produce the final CDK from the F.sub.3 result. At step 580, the ICP transmits the CDK to the playback device, which, at step 590, uses the CDK to decrypt the content.

The KDM (i.e. mating key) is used to identify the rights key, which is then used to transform the CDK and decrypt the content (i.e. decrypt the control word).

Regarding **Claim 1,** applicant's arguments have been fully considered but are not persuasive. With respect to applicants argument that "it is false to conclude that the KDM is generated using the rights key merely because it includes the CDK generator from which the CDK is derived," applicant is directed to Kocher, column 11- lines 40-63. As described above, Kocher discloses the rights keys (i.e. first derivative keys) are used to derive the CDK's which are a part of the KDM (i.e. mating key). Therefore, Kocher discloses the first derivative key is used to generate a mating key. Kocher further discloses the rights key includes a content identifier. Therefore, it is reasonable to read that the first derivative key (i.e. the rights keys) would be used to generate the mating key (i.e. KDM).

Regarding **Claim 13,** applicant's arguments have been fully considered but are not persuasive. With respect to applicants arguments that "the second value, allegedly KDM, is not recovered from a mating key generator undergoing a cryptographic operation using the first value, allegedly the rights key," applicant is directed to Kocher, column 8- lines 17-20, column 11- lines 38-40, Fig. 5. As stated above, Kocher discloses that the first derivative key would be used to generate the mating key. The REM (Rights Enablement Message) includes the rights key including an identifier of content. Kocher, column 11- lines 13-18, explicitly discloses:

> "The content identifier can be a simple identifier, a randomly produced or cryptographically generated value, a counter, a combination of parameters, etc. and may be generated by the content provider, ICP, playback device, CryptoFirewall, etc."

Therefore, the mating key generator is a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier, and a mating key sequence number.

Regarding **Claim 22,** applicant's arguments have been fully considered but are not persuasive. As discussed above, with respect to applicants argument that Kocher fails to teach *a second process block configured to generate a mating key from a mating*

key generator using the first derivative key, the mating key generator being a message that comprises at least one of a set-top-box manufacturer identifier, a service provider identifier, a conditional access (CA) provider identifier and a mating key sequence number. Applicant is directed to Kocher- column 11, lines 35-65, Fig. 2. Kocher discloses:

> FIG. 5 shows an exemplary method of the present invention for deriving CDKs using rights keys stored in the CryptoFirewall's protected memory. At step 500, the interface control processor (ICP) receives a key derivation message (KDM) from the playback device. At step 510, the ICP uses the KDM to obtain a CDK generator value. (The CDK generator is typically an encrypted form of the CDK and is part of the KDM.)

The rights keys (i.e. first derivative keys) are used to derive the CDK's which are a part of the KDM (i.e. mating key). Therefore, Kocher discloses the first derivative key is used to generate a mating key. Kocher further discloses the rights key includes a content identifier.

With respect to applicant's argument that Kocher fails to teach *a third process block configured to recover a control word by decrypting an encrypted control word*

using the mating key. Applicant is directed to Kocher- column 11, lines 48-65. Kocher discloses:

> The KDM also can identify which rights key is appropriate for processing each CDK generator.) At step 520, the CryptoFirewall verifies that the address is valid, then, at step 530, retrieves the corresponding value (the rights key) from the protected memory. At step 550, the CryptoFirewall uses pseudoasymmetric function F.sub.3, keyed with the rights key that was read from the protected memory at step 530, to transform the CDK generator. (In an alternate embodiment, F.sub.3 can be keyed with the CDK generator and used to transform the rights key itself. Also, F.sub.3 does not necessarily need to be a pseudoasymmetric or invertable function. For example, F3 can be a hash) At step 560, the CryptoFirewall returns the transformation result to the ICP. At step 570, the ICP optionally performs any final processing required to produce the final CDK from the F.sub.3 result. At step 580, the ICP transmits the CDK to the playback device, which, at step 590, uses the CDK to decrypt the content.

The KDM (i.e. mating key) is used to identify the rights key, which is then used to transform the CDK and decrypt the content (i.e. decrypt the control word).

With respect to applicant's argument that "the examiner alleges that the rights key corresponds to the first derivative key as well as the mating key generator," the rights key may be used to generate the mating key and can therefore be read to be a part of the mating key generation process. While the mating key generator and first derivative key are written as separate elements in the claim, Kocher discloses the rights key which successfully performs both functions.

From the examiner point of view the cited reference clearly teaches the limitations of the argued independent claims. The argued limitations (i.e. control word key ladder logic, first derivative key, mating key, mating key generator, control word), must be clearly defined in the claimed language, if applicant believes it differs from the cited art. Applicant is reminded that additional modification to clarify the claimed language is necessary for further consideration and distinction from the prior art. If

applicant feels the examiner is misinterpreting the claims and feels a telephone interview would resolve these issues, the examiner may be reached M-F: 8:00 - 4:00.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2435
2/19/2009

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2435